ValiCert

Digital Certificate Validation:
Technologies, Protocols and Infrastructure
Introduction to CRTs

Khaja E. Ahmed
khajaa@valicert.com
Director of Professional Services

Federal PKI TWG

May 13, 1999

Prologue

“Peter Williams of ValiCert, made a thought provoking presentation on online status protocols (TWG-99-25) and the Federal PKI. (…. Deleted ….) Peter contended that OCSP is about authoritative validation determinations, not simple status signaling, Peter introduced the concept of a "Validation Authority" (VA) that enables richer business models and added value services (such as insuring or guaranteeing particular transactions). Bill Burr observed that a logical conclusion of Peter's VA model is that an FPKI VA could (given suitable plug-ins for clients) entirely replace the BCA and it's cross certificates; that is the VA would collect revocation information from Federal CAs in accordance with the FPMA's determinations about the CAs and their policies, and issue authoritative validation responses to clients.”

Excerpt from Minutes of PKI TWG of April 99.

ValiCert

Certificate Validation Should

- Be Easy to use / be available

- Be Scaleable

- Be Cost effective

What does it take to deliver this?

Standards / Influencing factors

- Product Support, particularly browser adoption
- Standards Status
  - CRL, CDP -- PKIX
  - OCSP, CRTs -- OCSP
- Early Successes & Momentum
- Infrastructure / service availability

Standards / Technologies

- Certificate Revocation Lists (CRLs)
- CRL Distribution Points (CRL-DP)
- Online Certificate Status Protocol (OCSP)
- Certificate Revocation Trees (CRTs)

Characteristics

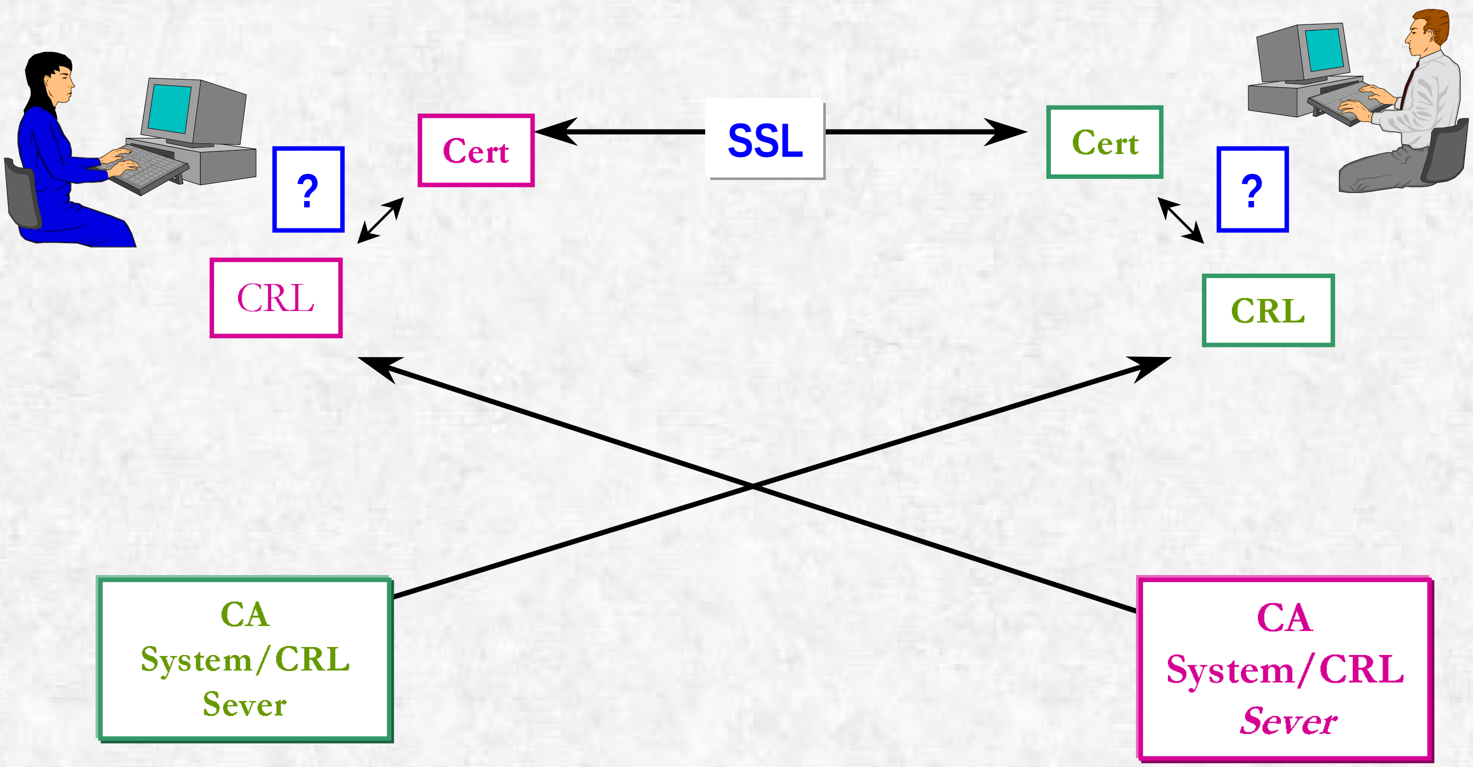
- Technology Approaches
- Product Support
- Applicability to E-Commerce Applications

Certificate Revocation List

- “Black List” of Revoked Certificates -- a negative file
- A Signed List
- Each Entry:
  - Serial Number of Certificate
  - Time of Revocation (e.g. Jan 15th, 1997 at 10:05 a.m.)
  - Other information (entry extensions) optional
    - e.g. Reason for revocation

76	5	2	19	24	Signature

Certificate Revocation List



ValiCert

What else is in a CRL?

- Issuer Name
  - Engineering Dept., ValiCert Inc., Mountain View, US
- Time of Issuance (thisUpdate)
- Time “at or before which new information will be available” (nextUpdate)
- Other Optional Information

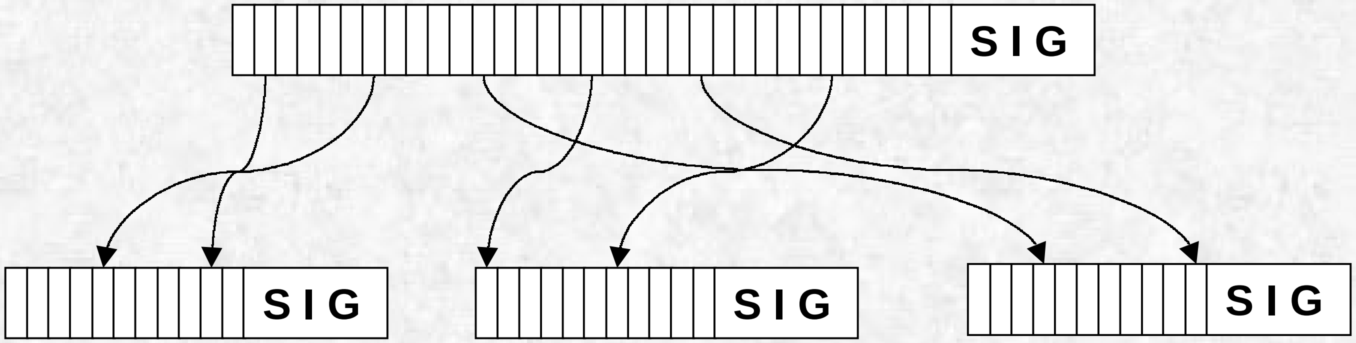
CRLs - Pros and Cons

- Application Checking Process
- Compatibility With Legacy Software
- Ability to Cache
- Size -- Storage, Network Bandwidth
- Requirement to Cache

ValiCert

CRL Distribution Points

- A clever mechanism to break up a CRL into smaller chunks



CRL Distribution Points

- Revocation Data is split into multiple buckets
- Each bucket is a “mini” CRL
- Every certificate contains data that allows applications to determine which bucket to look at to check validity.
    - May be more than one

ValiCert

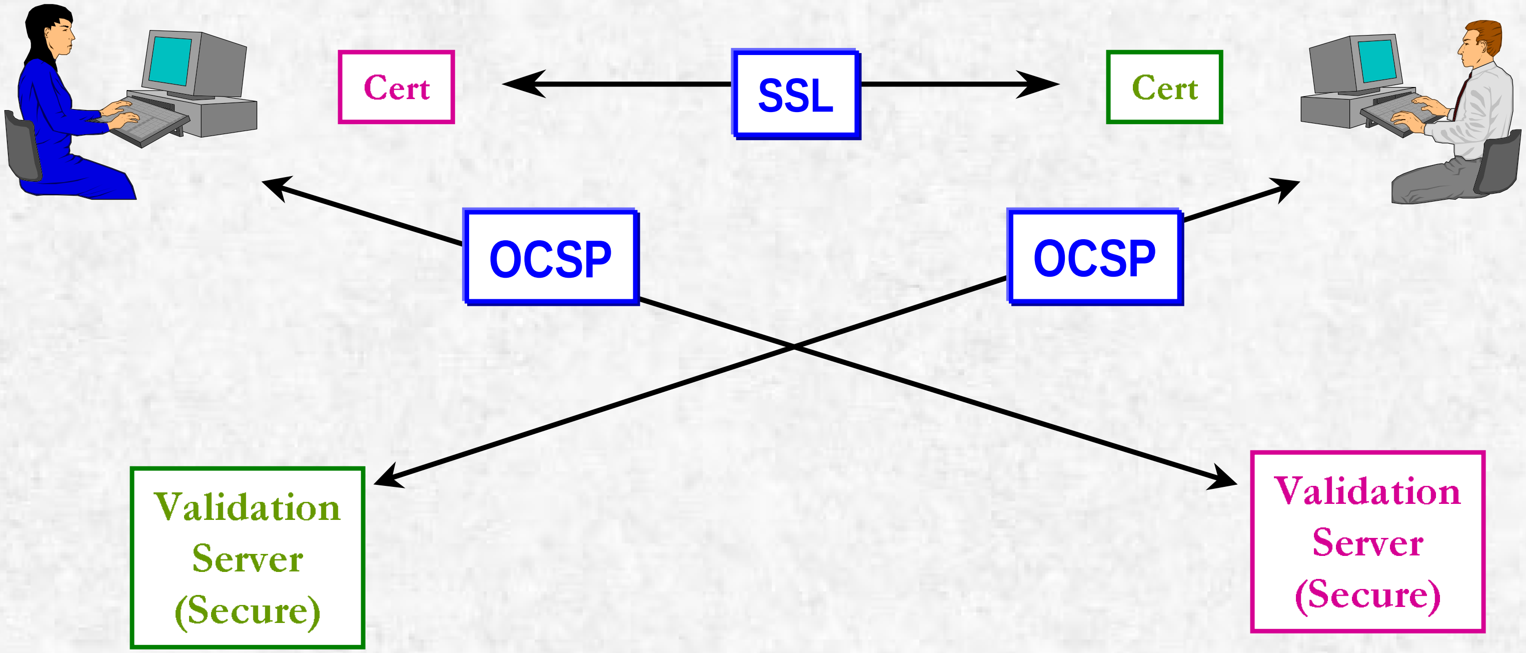
CRL Distribution Points -- Pros and Cons

- Application Checking Process
- Can be cached
- Requirement to be cached ameliorated
  - Reduces the size problem with CRLs
- Bucket for a certificate is fixed when it is issued
- Somewhat higher implementation complexity -- potential need to check multiple buckets (esp. forms based apps)

OCSP

- Online Certificate Status Protocol
- An “online” mechanism
- Simple Client-Server model
- Certificate accepting application (Client) asks OCSP Responder (Server) for a certificate’s status
- Server responds with yes (with time of revocation, reason for revocation), or no. The response is signed.

OCSP Model



ValiCert

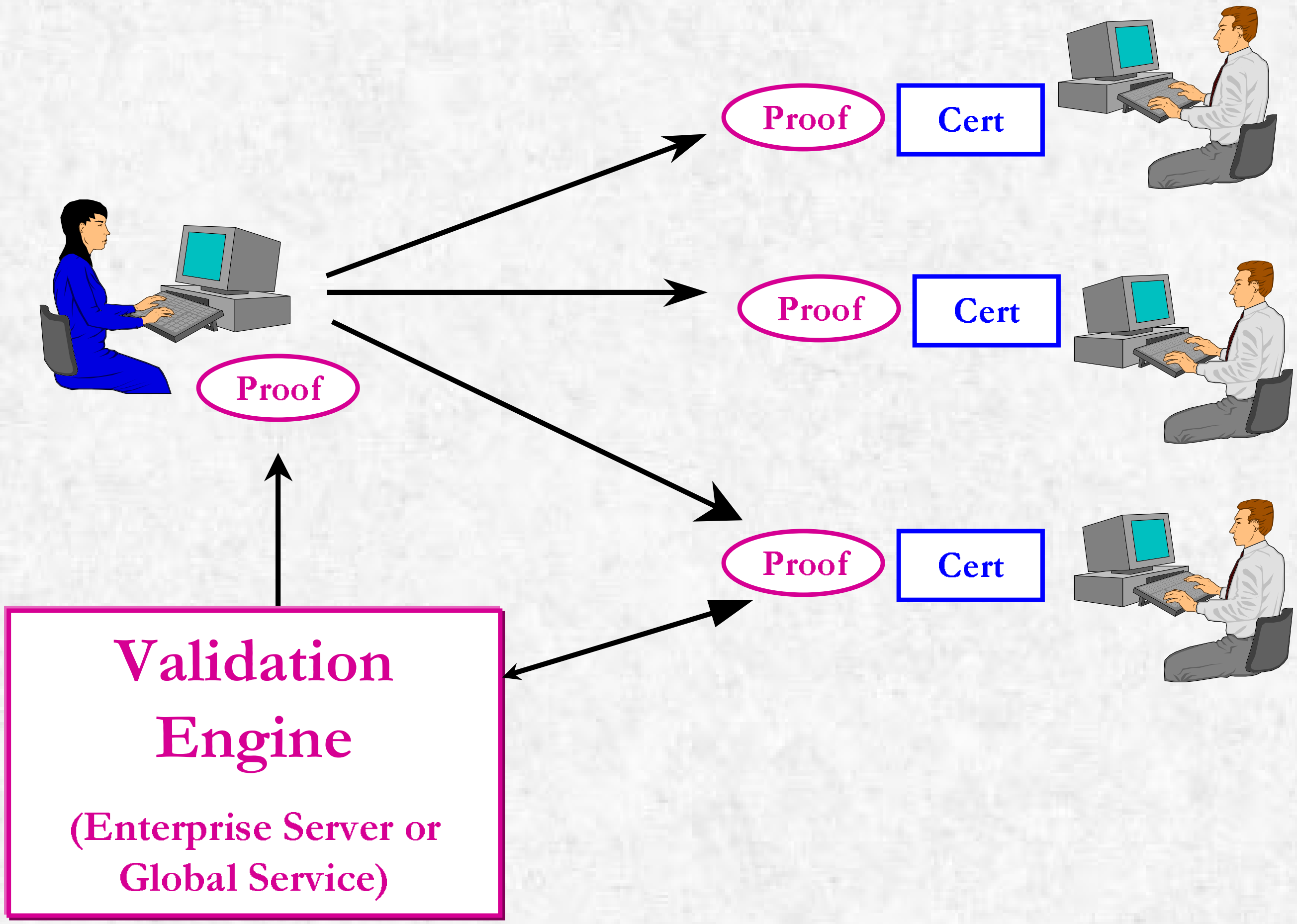
OCSP Pros and Cons

- Application Checking Process
- Up-to-Date Information
- Small Response Size
- Response may be Cached
- Responder needs to sign each response
- Responder key is online => must be in a secure site, introduces vulnerabilities / imposes costs
- Availability of service more limited

Certificate Revocation Trees

- Mechanism of revocation checking based on Merkle Hash Trees
- An on-line or off-line mechanism
- Client asks server if a certificate is valid
- Server provides a pre-signed piece of data, that client uses to decide if certificate is valid.
  - OCSP: RSA Signature, CRTs: Merkle Signature
  - OCSP: Signature on certificate, CRTs: Signature on range of certificates

The CRT Approach



Proof

Proof

Cert

Proof

Cert

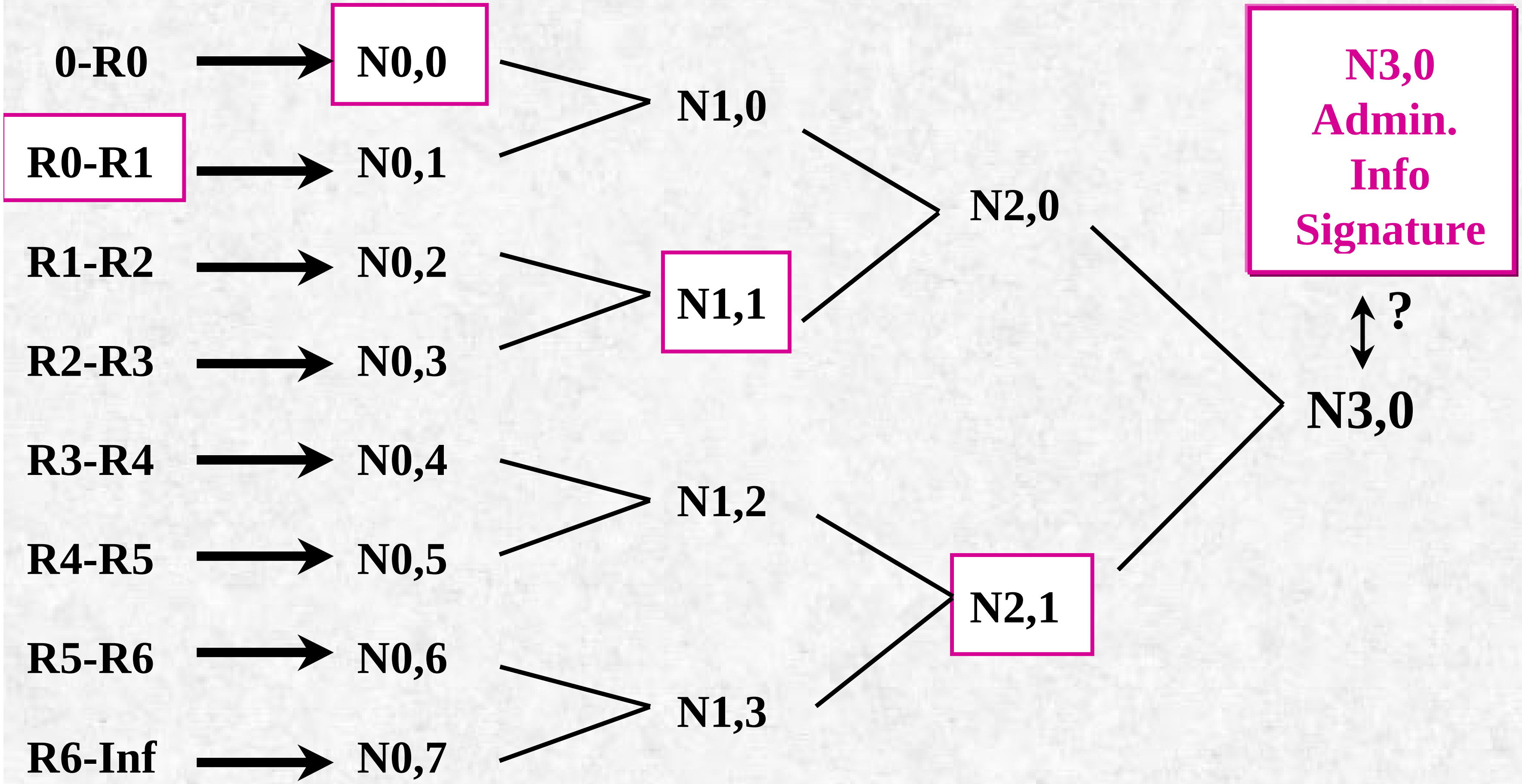
Proof

Cert

Validation Engine

(Enterprise Server or Global Service)

Certificate Revocation Trees



ValiCert

CRT Pros and Cons

- Size of responses much smaller than CDP/CRL but larger than OCSP responses
- No need to sign every response
- More secure (private key is not online)
- More scalable (each responder can support more clients)
- Tree building latency / distribution latency
- Response may be cached
- Can combine data from multiple CAs
- Easy and low cost distribution of responders

Product Support

	CRLs	CDPs	OCSP	CRTs
IE	☑	☑	Revocation DLLs	Revocation DLLs
Navigator	☑			
IIS			Plug-in	Plug-in
Suite Spot	Plug-in		Plug-in	Plug-in
Apache	Patches		Patches	Patches
Exchange			Plug-in	Plug-in
Other	Planned	Planned	Planned	Planned

ValiCert

Applicability to E-Commerce

CRLs work where...

- Size of Environment is Small
  - Intranets v/s Extranets or large commerce systems
- Frequent Updates not required
  - "regular" communication v/s mission-critical EDI
  - Security environment not super-sensitive
- Legacy application already support CRLs
- Caching not a problem
  - Desktop versus a smart card

Applicability to E-Commerce

CRL Distribution Points

- Desktop Applications versus a smart card.
- Updates frequent but not “online”
  - Mission critical Email/EDI, but not bond-purchase or stock-purchase.
- Much greater scalability and performance than CRLs but no business requirement to be online

Applicability to E-Commerce
OCSP

- Application MUST have data up to the last second
- Application IS online
- Application in a contained but large community where operation centers are manageable
  - Fed Reserve money supply management and international currency movement transactions and other multi-million dollar transactions

ValiCert

Applicability to E-Commerce
CRTs

- Application is used in small or large communities or open Internet
  - Secure Email, Brokerage
- Application may be used from desktop or Internet appliances
  - Secure Email, Brokerage
- Application may be online or offline
  - Secure Email
- Application needs security up to the minute but not up to the second.
  - Consumer Stock Brokerage but not FOMC trades

Which One(s) will win?

- The bottom-line:

One size does not fit all

- Off-line & On-line Applications
- Low security and high security applications
- Incompatibilities w/ product support
- Distributed and localized communities

ValiCert

Does It Matter?

- End-user software will need to support all major standards
  - Used in widely differing security environments
  - Used with different types of certificates
  - Used in very different E-Commerce situations
- Outsourcing Validation Services Far More Effective
  - Standards Translation
  - Cost Apportionment
  - Service Quality, Guarantees & Insurance
  - Ease of Set-Up

The ingredients for a complete revocation solution

- Validation server technology
- Validation clients / plug-ins to standard applications
- Technologies / tools to make applications validation aware in compliance with prevailing standards - (an API / toolkit)

What ties it all together...

- A VA network that spans and serves the globe
  - Ease of setup of interoperable trust
  - Scale to global use
- Fueled by CAs needing interoperability feeding revocation data to VAs to our-source validation

Epilogue….

- A global network of VAs (Validation Authorities) that are multi protocol capable and CA independent will emerge.
- Most E-Commerce applications that need online approaches will use OCSP with high-performance add-ons like CRTs
- CRTs will be used for scalability and performance
  - total cost of ownership versus benefit of reduction of security risk

Summary

- 4 major approaches
  - CRLs, CRL DPs, OCSP & CRT
- One Size Does Not Fit All --Need for multiple approaches & interoperability.
- Validation Authority network will be multi protocol capable and provide a global infrastructure for real time, online, scalable validation to enable e-commerce